Chapter 4

Information Systems Safeguards

Left blank intentionally

4-1 Information Systems Safeguards

Overview

1. This chapter specifies security safeguards for the protection of FEMA's information systems. The security controls, procedures, and documentation standards establish the MINIMUM requirements for safeguarding classified and unclassified information technology hardware and software assets. The increased use of electronic media to store, process and transmit information adds a new dimension of complexity to traditional security concerns.

2. Managers at every level play lead roles in information security. Even program or functional managers, who do not oversee general support systems or major applications, have responsibility for providing information safeguards: managerial, operational, and technical. Integrating security safeguards into every phase of the program's life cycle is essential for protecting the confidentiality, integrity, and availability of information resources used in support of FEMA's mission.

3. As in other aspects of sound management, cost containment is a major part of information security. Experience has shown that costs are lower and risks are lessened when information safeguards are incorporated into the design and development of information systems. However, incorporating information safeguards into the design specifications does not negate the need for periodic assessments as threats change over time, and subsequent systems updates may alter the nature of the security environment.

Responsibility

1. The Chief Information Officer is responsible for:

   - Overseeing FEMA's information systems security policy, procedures, and practices.
   - Identifying and affording security protections commensurate with the risk and magnitude of the harm that may result from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of the Agency.
   - Appointing FEMA's Enterprise Security Manager.
   - Overseeing development and implementation of FEMA's information security training program.
   - Approving recommendations for application systems security accreditation.

2. Executive Associate Director, Information Technology Services Directorate is responsible for:

   - Developing and implementing applicable information systems policy, procedures, standards, and guidelines on privacy, confidentiality, security, disclosure, and sharing of information collected, processed, transmitted, or maintained by or for the Agency.

   - Coordinating with the Executive Associate Director, Operations Support Directorate, on all security matters pertaining to classified and sensitive unclassified information systems.

3. Associate Directors, Administrators, Executive Associate Directors, Regional Directors, and Office Directors are responsible for:

   - Ensuring FEMA’s information systems security policy, requirements, and guidelines are followed in developing system specifications and contracts for the acquisition or operation of information systems, associated resources, and facilities.

   - Issuing, for programs and functions under their purview, information systems safeguards beyond the Agency’s minimum stated requirements, as required.

   - Assigning security personnel, Site Mangers/Administrators and/or Network Administrators, as required.

   - Conducting effective security certification and accreditation for major, mission critical, high risk, financial, or classified information systems.

   - Authorizing information systems and by implication accepting the risks extant in the systems.

   - Implementing controls consistent with the criticality, value, and sensitivity of the information being handled.

   - Ensuring that employees are made aware of all information security policies and procedures and that security training is available for users, custodians, and owners of sensitive FEMA information assets.

4. The Inspector General is responsible for:

   - Performing independent audits relating to information systems security, including assessing compliance with information systems security and privacy legislation, regulations, and requirements.

- Assisting the CIO and the Director, Security Division of the Operations Support Directorate, in information systems security investigations; or as appropriate, conducting criminal investigations and making referrals to the United States Department of Justice.

5. The FEMA Enterprise Security Manager is responsible for:

- Approving the acquisition, configuration and installation of routers, switches, firewalls and other network-related equipment.
- Assuring FEMA information assets are used only for FEMA purposes.
- Assuring compliance with all applicable State and Federal laws and administrative policies.
- Assuring compliance with security policies and procedures established by the owners of the information assets and by the FEMA CIO.
- Advising the owner of information and the CIO of any vulnerability presenting a threat to information assets, and for providing specific means of protecting that information.
- Notifying the owner of information and the CIO of any actual or attempted violations of security policies, practices or procedures.
- Approving the addition of Local Area Network (LAN) or Wide Area Network (WAN) devices that impact Internet or Intranet services.
- Establishing and approving the security configuration control of all network devices.
- Developing or assisting with the development of operational procedures.
- Assuring adherence to all FEMA WAN-naming conventions.
- Developing or assisting with the development of operational procedures.
- Assuring adherence to all FEMA WAN-naming conventions.
- Providing support for the issuance of hardware tokens and maintenance of authentication databases.
- Evaluating vendor security products and apprising the Agency of approved Information Technology (IT) security products and techniques.
- Developing security accreditation guidelines and procedures for new application development.

- Participating as technical security advisor on in-house system development projects and assisting with security control implementations.
- Performing independent audits relating to information systems security, including assessing compliance with information systems security and privacy legislation, regulations and requirements.
- Conducting pre-production security tests to ensure compliance with FEMA security practices for new applications and devices.
- Investigating reports of information systems security compromises, violations or breaches, and recommending or implementing security countermeasures or corrective actions, as appropriate.
- Performing other security duties as assigned.

6. The Site Manager/Administrator has overall responsibility for:

- Managing the local networks at a location where there are multiple local area networks with different Network Administrators.
- Ensuring security, integrity, availability, and confidentiality of local information systems and network services for the site.
- Presenting security orientations to current employees and new hires.
- Processing newly arriving and departing employees to ensure compliance with security procedures, as required in Chapter 4-4 under “Personnel Security and Control” and “Access Control” headings.

7. The Network Administrator is responsible for:

- Establishing and maintaining configuration, operation and security of the local system.
- Maintaining the configuration management of all hardware and software connected to the local network.
- Ensuring that system/network users comply with IT security policies and procedures.
- Reviewing and auditing the information system/network on a regular basis to determine that the network remains secure.
- Reporting any suspected security incidents to FEMA’s Information Technology Service Center (ITSC) at Mt. Weather (540) 542-4000 or directly to the ESM.

- Ensuring the integrity of program data through regularly scheduled system backups and any required restorations.

8. The Information Technology Service Center (ITSC), which is located at Mt. Weather, is responsible for:

   - Providing 24-hour-a-day, 7-day-a-week help desk for users of FEMA's information systems during declared disasters. At other times, the ITSC operates 16 hours a day. The ITSC can be reached on (540) 542-4000.
   - Taking reports on and processing suspected or actual network security problems.
   - Notifying the ESM and appropriate system/network administrator immediately following the reported incident.

Procedures

The procedures for information systems safeguards cover three levels of activities: user requirements, general support systems requirements, and applications systems.

1. User requirements describe the information safeguards to be practiced by users needed for routine administrative and program activities within an office environment. As the procedures represent only the minimal security safeguards, FEMA managers are authorized to impose additional safeguards if the sensitivity of the data warrants additional protection.

2. A general support system is defined as an interconnected set of information resources under the same direct management control; the systems provide processing or communications support or some combination thereof. For purposes of this directive, FEMA network administrators shall adhere to the security safeguards listed in Chapter 4-3 for general support systems.

3. Applications systems require additional security measures and oversight throughout their life cycles. A major application is defined as a large investment, mission critical, cross cutting or high risk use of information and information technology to satisfy a specific set of agency requirements. A major application requires management attention to security due to the risk and magnitude of harm that would result from loss, misuse, or unauthorized access to or modification of the information in the application.

Left blank intentionally

4-2 System User Security Requirements

Overview

1. This chapter specifies security safeguards for the protection of FEMA's information systems. The security controls, procedures, and documentation standards establish the MINIMUM requirements for safeguarding classified and unclassified information technology hardware and software assets. The increased use of electronic media to store, process and transmit information adds a new dimension of complexity to traditional security concerns.

2. Managers at every level play lead roles in information security. Even program or functional managers, who do not oversee general support systems or major applications, have responsibility for providing information safeguards: managerial, operational, and technical. Integrating security safeguards into every phase of the program's life cycle is essential for protecting the confidentiality, integrity, and availability of information resources used in support of FEMA's mission.

3. As in other aspects of sound management, cost containment is a major part of information security. Experience has shown that costs are lower and risks are lessened when information safeguards are incorporated into the design and development of information systems. However, incorporating information safeguards into the design specifications does not negate the need for periodic assessments as threats change over time, and subsequent systems updates may alter the nature of the security environment.

4. Magnetic media and other types of media used to store software and data at user workstations must be protected. Inadequate protection or improper handling of storage media such as diskettes, tape cassettes, fixed hard disks, and removable hard disks may result in the loss of valuable software or data, or lead to unauthorized disclosure or modification of data.

5. Computer viruses represent a serious computer security problem that can cause a wide variety of disruptive or destructive actions on systems. For instance, viruses may corrupt or totally destroy data residing on storage media or cause computer hardware or software damage. In view of the increasing risk of computer viruses, all FEMA PCs and networked PCs shall be tested for and protected against viral infection.

Responsibility

1. The Chief Information Officer is responsible for:

    - Overseeing FEMA's information systems security policy, procedures, and practices.

- Identifying and affording security protections commensurate with the risk and magnitude of the harm that may result from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of the Agency.
- Appointing FEMA’s Enterprise Security Manager.
- Overseeing development and implementation of FEMA’s information security training program.
- Approving recommendations for application systems security accreditation.

2. Executive Associate Director, Information Technology Services Directorate is responsible for:

   - Developing and implementing applicable information systems policy, procedures, standards, and guidelines on privacy, confidentiality, security, disclosure, and sharing of information collected, processed, transmitted, or maintained by or for the Agency.
   - Coordinating with the Executive Associate Director, Operations Support Directorate, on all security matters pertaining to classified and sensitive unclassified information systems.

3. Associate Directors, Administrators, Executive Associate Directors, Regional Directors, and Office Directors are responsible for:

   - Ensuring FEMA’s information systems security policy, requirements, and guidelines are followed in developing system specifications and contracts for the acquisition or operation of information systems, associated resources, and facilities.
   - Issuing, for programs and functions under their purview, information systems safeguards beyond the Agency’s minimum stated requirements, as required.
   - Assigning security personnel, Site Mangers/Administrators and/or Network Administrators, as required.
   - Conducting effective security certification and accreditation for major, mission critical, high risk, financial, or classified information systems.
   - Authorizing information systems and by implication accepting the risks extant in the systems.
   - Implementing controls consistent with the criticality, value, and sensitivity of the information being handled.

- Ensuring that employees are made aware of all information security policies and procedures and that security training is available for users, custodians, and owners of sensitive FEMA information assets.

4. The Inspector General is responsible for:

- Performing independent audits relating to information systems security, including assessing compliance with information systems security and privacy legislation, regulations, and requirements.
- Assisting the CIO and the Director, Security Division of the Operations Support Directorate, in information systems security investigations; or as appropriate, conducting criminal investigations and making referrals to the United States Department of Justice.

5. The FEMA Enterprise Security Manager is responsible for:

- Coordinating the provision of security for Agency automated information systems and networks.
- Security, integrity, and availability of information system services and networks that support FEMA operations.
- Assessing security risks and vulnerability threats to FEMA information assets and providing specific means of protecting those information systems.
- Evaluating vendor security products and apprising the Agency of approved IT security products and techniques.
- Obtaining and assessing information systems security accreditation evidence as the basis for recommending security accreditation to the CIO.
- Ensuring that appropriate security controls are installed, operated, and maintained to protect FEMA information assets.
- Investigating reports of information systems security compromises, violations, or breaches, and recommending security countermeasures or corrective actions in coordination with the Operations Support Directorate and the Office of Inspector General.
- Reviewing the configurations of all Agency information systems hardware and software.
- Ensuring that network security complies with applicable State and Federal laws and regulations, and with Agency policies and procedures.

- Participating as technical security advisor on in-house system development projects and assisting with security control implementations.
- Establishing and reviewing security configurations of all network devices.
- Assisting with the development of operational security practices.
- Ensuring adherence to all FEMA network-naming conventions.
- Providing support for the issuance of hardware tokens and maintenance of authentication databases.

6. The Site Manager/Administrator has overall responsibility for:

- Managing the local networks at a location where there are multiple local area networks with different Network Administrators.
- Ensuring security, integrity, availability, and confidentiality of local information systems and network services for the site.
- Presenting security orientations to current employees and new hires.
- Processing newly arriving and departing employees to ensure compliance with security procedures, as required in Chapter 4-4 under “Personnel Security and Control” and “Access Control” headings.

7. The Network Administrator is responsible for:

- Establishing and maintaining configuration, operation and security of the local system.
- Maintaining the configuration management of all hardware and software connected to the local network.
- Ensuring that system/network users comply with IT security policies and procedures.
- Reviewing and auditing the information system/network on a regular basis to determine that the network remains secure.
- Reporting any suspected security incidents to FEMA’s Information Technology Service Center (ITSC) at Mt. Weather (540) 542-4000 or directly to the ESM.
- Ensuring the integrity of program data through regularly scheduled system backups and any required restorations.

8. The Information Technology Service Center (ITSC), which is located at Mt. Weather, is responsible for:

   - Providing 24-hour-a-day, 7-day-a-week help desk for users of FEMA's information systems during declared disasters. At other times, the ITSC operates 16 hours a day. The ITSC can be reached on (540) 542-4000.

   - Taking reports on and processing suspected or actual network security problems.

   - Notifying the ESM and appropriate system/network administrator immediately following the reported incident.

Procedures

Workstation Controls

Information security encompasses basic physical protection for resources entrusted to users care. Inadequate physical security may lead to theft, damage, or the destruction of hardware, software, and storage media. Additionally, lack of controls may result in the unauthorized disclosure, modification, or destruction of data resident on the system.

1. Protect workstations against unauthorized access. Use appropriate access control measures and follow established control procedures. Physical access controls are essential when authorized personnel cannot effectively monitor equipment.

2. Ensure that unauthorized personnel are not able to view sensitive data displayed at a workstation.

3. Monitor the printer to prevent unauthorized disclosure when printing sensitive data.

4. Remove sensitive output from the printer or other output device connected to the system as soon as possible. Delay may lead to unauthorized access.

Software & Data Controls

The following administrative control requirements are applicable to all users operating workstations in unclassified environments:

1. Do not originate, process, store, or transmit classified data on a system designated for unclassified use.

2. Do not use the workstation for personal business or entertainment.

3. Do not copy software from FEMA's workstations for use on privately owned computers, unless allowed by the software license, used only for official business, and authorized by management.

4. Do not copy FEMA data for use on privately owned computers unless authorized by management.

5. Do not install or use privately owned software on a workstation or upload privately owned software to software directories on a file server unless specifically authorized by the Enterprise Security Manager, checked for computer viruses, and used only for official business.

6. Do not process or store privately owned data on a workstation or file server.

7. Use proprietary software and related documentation in conformance with copyright restrictions, licenses, and other legal agreements. The duplication of proprietary software and documentation, except for backup purposes, is prohibited, unless permitted by the license and authorized by management.

8. Obtain written authorization before removing hardware, software, or documentation from a FEMA facility.

9. Report theft, damage, misuse, and unauthorized access of hardware, software, or data.

Downloading and Storing Data at Workstations

1. Safeguard data when downloading data from a FEMA file server for local use and storage at a workstation. Data that may be adequately protected on a file server may be extremely vulnerable to unauthorized access when stored on a fixed disk at a workstation.

2. Safeguard networks, hardware, software, and data when downloading executable programs or data from the Internet for local use and storage at a workstation. For computer virus protection see below.

3. For sensitive data, store data on removable media and physically protect the media from unauthorized access by storing the media in a locked desk, locked cabinet, safe, or other secure location.

Storage Media Protection

1. Protect diskettes and other types of removable storage media against unauthorized access, loss, and destruction.

2. Store diskettes and other types of removable storage media containing sensitive or critical data in locked desks, locked cabinets, safes, or locked rooms.

3. Label all removable storage media used at a workstation.

4. Use SF 710, Unclassified Label, to label unclassified removable media when unclassified and classified media are used or stored in the same [room or container] area.

5. Identify data stored on the media and indicate the sensitivity of data (e.g., Privacy Act data), if appropriate.

6. Exercise care when handling diskettes. Read and follow proper handling procedures for storage media.

7. Dispose of old or unwanted diskettes and tape cassettes that contain sensitive data by cutting into small pieces, shredding, burning, or using other methods of destruction that prevent unauthorized disclosure of data.

Backup

Each user is responsible for making and safeguarding backup copies of files residing on local storage media used at workstations. Current and reliable backup copies of word processing files and data files provide insurance against the loss of valuable or critical information system assets.

1. Make regular and systematic backup copies of word processing and data processing files resident on local storage media at workstations.

2. Comply with backup requirements specified by management.

3. Label and date all backup media used at a workstation so backup data can be readily identified and loaded when needed.

4. Protect backup media in the same manner as media containing original word processing and data files.

Computer Viruses on PCs and LANs

1. Protect workstations against computer viruses by using antivirus software tested and issued by the Information Technology Services Directorate, Operations Division.

2. Contact the ITS Operations Division for assistance in using the antivirus software or to report problems with the software package.

3. Do not install any software on a workstation or file server unless the software has been authorized and tested for virus infection. Public domain software, shareware, freeware, computer games, and software copied from a home system or another user's system may be infected with a virus or contain other malicious code that may infect a workstation or the entire network.

4. Report virus incidents immediately whenever any unusual activity occurs at a workstation or a computer virus is suspected or detected.

Left blank intentionally

4-3 General Support Systems Safeguards

Overview

1. This chapter specifies security safeguards for the protection of FEMA's information systems. The security controls, procedures, and documentation standards establish the MINIMUM requirements for safeguarding classified and unclassified information technology hardware and software assets. The increased use of electronic media to store, process and transmit information adds a new dimension of complexity to traditional security concerns.

2. Managers at every level play lead roles in information security. Even program or functional managers, who do not oversee general support systems or major applications, have responsibility for providing information safeguards: managerial, operational, and technical. Integrating security safeguards into every phase of the program's life cycle is essential for protecting the confidentiality, integrity, and availability of information resources used in support of FEMA's mission.

3. As in other aspects of sound management, cost containment is a major part of information security. Experience has shown that costs are lower and risks are lessened when information safeguards are incorporated into the design and development of information systems. However, incorporating information safeguards into the design specifications does not negate the need for periodic assessments as threats change over time, and subsequent systems updates may alter the nature of the security environment.

4. One major aspect of computer system security is controlling access to FEMA systems, networks, files and databases. Access to a system is strictly controlled to prevent the unauthorized disclosure, modification, or destruction of data and program files resident on the system storage devices. To protect against unauthorized access, FEMA assigns unique user identifiers (user IDs) and passwords to identify and authenticate authorized users. User IDs also play a key role in authorizing and controlling access to programs and data resident on the system, as well as ensuring individual user accountability on the system.

5. Standards and naming conventions for developing and assigning unique user IDs will be provided in Chapter 5 of this directive. The following sections describe FEMA standard practices in controlling these areas.

Responsibility

1. The Chief Information Officer is responsible for:

   - Overseeing FEMA's information systems security policy, procedures, and practices.

- Identifying and affording security protections commensurate with the risk and magnitude of the harm that may result from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of the Agency.
- Appointing FEMA's Enterprise Security Manager.
- Overseeing development and implementation of FEMA's information security training program.
- Approving recommendations for application systems security accreditation.

2. Executive Associate Director, Information Technology Services Directorate is responsible for:

- Developing and implementing applicable information systems policy, procedures, standards, and guidelines on privacy, confidentiality, security, disclosure, and sharing of information collected, processed, transmitted, or maintained by or for the Agency.
- Coordinating with the Executive Associate Director, Operations Support Directorate, on all security matters pertaining to classified and sensitive unclassified information systems.

3. Associate Directors, Administrators, Executive Associate Directors, Regional Directors, and Office Directors are responsible for:

- Ensuring FEMA's information systems security policy, requirements, and guidelines are followed in developing system specifications and contracts for the acquisition or operation of information systems, associated resources, and facilities.
- Issuing, for programs and functions under their purview, information systems safeguards beyond the Agency's minimum stated requirements, as required.
- Assigning security personnel, Site Mangers/Administrators and/or Network Administrators, as required.
- Conducting effective security certification and accreditation for major, mission critical, high risk, financial, or classified information systems.
- Authorizing information systems and by implication accepting the risks extant in the systems.
- Implementing controls consistent with the criticality, value, and sensitivity of the information being handled.

- Ensuring that employees are made aware of all information security policies and procedures and that security training is available for users, custodians, and owners of sensitive FEMA information assets.

4. The Inspector General is responsible for:

- Performing independent audits relating to information systems security, including assessing compliance with information systems security and privacy legislation, regulations, and requirements.
- Assisting the CIO and the Director, Security Division of the Operations Support Directorate, in information systems security investigations; or as appropriate, conducting criminal investigations and making referrals to the United States Department of Justice.

5. The FEMA Enterprise Security Manager is responsible for:

- Approving the acquisition, configuration and installation of routers, switches, firewalls and other network-related equipment.
- Assuring FEMA information assets are used only for FEMA purposes.
- Assuring compliance with all applicable State and Federal laws and administrative policies.
- Assuring compliance with security policies and procedures established by the owners of the information assets and by the FEMA CIO.
- Advising the owner of information and the CIO of any vulnerability presenting a threat to information assets, and for providing specific means of protecting that information.
- Notifying the owner of information and the CIO of any actual or attempted violations of security policies, practices or procedures.
- Approving the addition of Local Area Network (LAN) or Wide Area Network (WAN) devices that impact Internet or Intranet services.
- Establishing and approving the security configuration control of all network devices.
- Developing or assisting with the development of operational procedures.
- Assuring adherence to all FEMA WAN-naming conventions.
- Developing or assisting with the development of operational procedures.

- Providing support for the issuance of hardware tokens and maintenance of authentication databases.

- Evaluating vendor security products and apprising the Agency of approved Information Technology (IT) security products and techniques.

- Developing security accreditation guidelines and procedures for new application development.

- Participating as technical security advisor on in-house system development projects and assisting with security control implementations.

- Performing independent audits relating to information systems security, including assessing compliance with information systems security and privacy legislation, regulations and requirements.

- Conducting pre-production security tests to ensure compliance with FEMA security practices for new applications and devices.

- Investigating reports of information systems security compromises, violations or breaches, and recommending or implementing security countermeasures or corrective actions, as appropriate.

6. The Site Manager/Administrator has overall responsibility for:

   - Managing the local networks at a location where there are multiple local area networks with different Network Administrators.

   - Ensuring security, integrity, availability, and confidentiality of local information systems and network services for the site.

   - Presenting security orientations to current employees and new hires.

   - Processing newly arriving and departing employees to ensure compliance with security procedures, as required in Chapter 4-4 under “Personnel Security and Control” and “Access Control” headings.

7. The Network Administrator is responsible for:

   - Establishing and maintaining configuration, operation and security of the local system.

   - Maintaining the configuration management of all hardware and software connected to the local network.

   - Ensuring that system/network users comply with IT security policies and procedures.

- Reviewing and auditing the information system/network on a regular basis to determine that the network remains secure.

- Reporting any suspected security incidents to FEMA's Information Technology Service Center (ITSC) at Mt. Weather (540) 542-4000 or directly to the ESM.

- Ensuring the integrity of program data through regularly scheduled system backups and any required restorations.

8. The Information Technology Service Center (ITSC), which is located at Mt. Weather, is responsible for:

   - Providing 24-hour-a-day, 7-day-a-week help desk for users of FEMA's information systems during declared disasters. At other times, the ITSC operates 16 hours a day. The ITSC can be reached on (540) 542-4000.

   - Taking reports on and processing suspected or actual network security problems.

   - Notifying the ESM and appropriate system/network administrator immediately following the reported incident.

Procedures

Access Control - System Accounts

1. In order to obtain a user account on any FEMA computer system, a request will be submitted through the supervisor to the Network Administrator who reviews the levels of system and database access. Both the Network Administrator and the appropriate application Data Base Administrator will implement such requests. Further reference material for Disaster Field Office's Network Administrator is provided in Appendix 4.3.c, "Disaster Field Officer's Network Administrators Guide."

2. Telephone discussions involving sensitive or classified U.S. Government Information must be conducted using a Secure Telephone Unit "STU-III" and the proper safeguards provided in FEMA Manual 1550.3.

3. Up-to-date account information must be maintained and monitored for inactivity. Account inactivity exceeding 30 days should warrant an inquiry. Failure to respond to a revalidation inquiry should justify account suspension.

4. Group accounts or shared passwords are prohibited. Any variance from this standard practice must be documented and waived by the Network Administrator in coordination with the Enterprise Security Manager and program or system manager.

Access Control - Account Termination

1. Accounts may be frozen due to extended leaves of absence, investigations, temporary assignments, etc.

2. Accounts must be terminated when an employee leaves FEMA, is reassigned, or no longer requires access. Supervisors are required to notify the cognizant Network Administrator when an employee no longer requires access.

Access Control - Password Management

1. Never disclose passwords to anyone or write them down on any medium accessible to others. Users are responsible for actions and events resulting from the disclosure of personal passwords.

2. Never store the network log-in command or a server attach command along with a user ID and password in a batch file on a workstation or in a user log-in script stored on a file server. This practice constitutes a serious vulnerability; it creates an easily accessible path for unauthorized access.

3. Report suspected password compromises.

4. Comply with the following requirements if the security system permits users to change personal passwords:

   - Change passwords at least every ninety (90) days to protect against undetected password compromise;

   - Change passwords whenever password compromises are suspected;

   - Avoid choosing passwords that incorporate personal information (e.g., users' names, children's names, dates of birth, addresses, telephone numbers, etc.); Passwords must NOT be related to the user's job or personal life, or words found in the dictionary. For example, car license plate number, spouse's name, address, proper names, places, and slang terms should not be used.

   - Choose passwords that are at least eight alphanumeric characters in length with at least one non-alphabetic character such as a numeral (0-9) or punctuation character. One recommended format for passwords is CVCNNCVC, where C is a consonant, V is a vowel, and N is a numeral (e.g., BAT56ZAM).

5. If system generated passwords are used, they must be generated using the low order bits of the system clock or some other unpredictable source. So that users can more easily remember them, and so that users will not need to write them down; all system-generated

passwords for end-users must be pronounceable. Passwords or Personal Identification Numbers (PINs) that are generated by a computer system must be issued immediately after they are generated. Regardless of the form they take, unissued passwords and PINs must never be stored on the computer systems unless they are encrypted.

6. Initial passwords issued by a Network Administrator will be valid only for the user's first on-line session. Users will be automatically notified and required to change their passwords at least once every ninety (90) days.

7. Consecutive entry of the incorrect password will be strictly limited. After three (3) unsuccessful attempts to enter a password, the user ID will be either (a) suspended until reset by the Network Administrator, (b) temporarily disabled for not less than three (3) minutes, or (c) if dial-up or other external network connections are involved, disconnected.

8. When the system is compromised or there is a suspicion of compromise, the Network Administrator will immediately change every password on the system. A trusted version of the operating system and all security-related software must also be reloaded. All recent changes to user and system privileges should be reviewed for unauthorized modifications.

9. When an employee who had system privileges and access to password files leaves FEMA or is no longer in a position of trust, all systems to which the employee had access must be notified and passwords must be changed.

Log-in Process

1. All users must be identified prior to being able to use any multi-user computer or communications system resources. All users must have their identity verified with a user-ID and a private password or by other means that provide equal or greater security-prior to being permitted to use FEMA computers connected to a network.

2. Remote access to FEMA systems via dial-in modems will require the use of a strong authentication system employing a hardware token when they become available. The use of the hardware token applies to all dial-in connections. The hardware token will be used to generate a one-time password unique to that log-in session.

3. All log-in banners on network-connected FEMA computer systems will require the user to log-in, providing prompts as needed. Specific information about the organization, the computer operating system, the network configuration, or other internal matters must not be provided in the log-in banner until a user has successfully provided both a user-ID and a password. When logging into a FEMA computer or data communications system, if any part of the log-in sequence is incorrect, the user will not be given specific feedback indicating the source of the problem. Instead, the user will be informed that the log-in process was incorrect after all of the log-in information has been entered.

4. The log-in process on multi-user computers will include a special notice: (1) the system is to be used only by authorized users, (2) this session may be monitored by FEMA management, and (3) by continuing to use the system, the user represents that he/she is an authorized user.

5. Users will be given information reflecting the last log-in time and date, which will allow detection of unauthorized system usage.

Log-off Process

1. Users must not leave their microcomputer (PC), workstation, or terminal unattended without first logging-out.

2. Inactivity on a computer terminal, workstation, or microcomputer for ten (10) minutes will cause the system to automatically blank the screen and suspend the session. Re-establishment of the session must take place only after the user has provided the proper password.

Privilege Control - Level of Access

1. The computer and communications system privileges of all users, systems, and programs will be based on the need-to-know. All computer-resident information that is either private, restricted, or sensitive will have system access controls to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable.

2. Access controls should be consistent with the information being protected and the computer system hosting the data. Access controls typically consist of Access Control Lists or other mechanisms that limit users' ability to read, modify, or delete information in accordance with their need-to-know.

3. Firewalls should protect servers that store and process sensitive data because the unauthorized modification, deletion, or release of sensitive data would have severe consequences. Refer to Appendix 4-3.A, Firewall Management and Administration, for further information.

Privilege Control - Logging and Auditing

1. System logs and audit trails, appropriate for the value of the system protected, will be maintained for each FEMA information asset to correct problems encountered due to intentional or inadvertent misuse.

2. All production application systems that handle private, restricted or sensitive FEMA information must generate logs that show every addition, modification, and deletion to such sensitive information. Any systems that do not support such logging capabilities must maintain a documented requirements analysis, approved by the applicable program manager, that justifies such operation. Mechanisms to detect and record significant computer security events must be resistant to attacks. These attacks include attempts to deactivate, modify, or delete the logging software and/or the logs themselves.

3. All FEMA computer systems connected to networks will securely log all significant computer security relevant events. Examples of computer security relevant events include: password guessing attempts, attempts to use privileges that have not been authorized, modifications to production application software, and modifications to system software. Logs of computer security relevant events must provide sufficient data to support comprehensive audits of the effectiveness of, and compliance with security measures.

4. All commands issued by computer system operators will be traceable to specific individuals via the use of comprehensive logs. Logs of major computer security relevant events must be retained for at least three (3) months. During this period, logs must be secured such that they cannot be modified, and such that only authorized persons can read them. All system and application logs must be securely maintained and accessible only on a need-to-know basis.

5. To allow proper remedial action, computer operations or information security staff must review records reflecting security relevant events in a periodic and timely manner. The Network Administrator and Enterprise Security Manager must review logs on a weekly basis. Where incidents of misuse or abuse are detected, procedures defined for incident reporting and handling must be followed.

<u>Virus Prevention and Detection</u>

1. A computer virus is an unauthorized program that replicates itself and spreads onto various data storage media (floppy disks, magnetic tapes, disk drives, etc.) and/or across a network. The symptoms of virus infection include much slower computer response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total failure of computers.

2. FEMA employees are cautioned to be especially careful when downloading software from electronic bulletin board systems, external communication networks, or other systems outside FEMA, to include the Internet and the World Wide Web. This caution is necessary because such software may contain viruses and may damage FEMA information and systems. All new software to be introduced into the FEMA system must be scanned for viruses.

3. Every computer connected to a FEMA network will use virus detection software that will automatically scan upon startup, floppy disk insertion, and on any file storage operation. FEMA’s agency-wide standard anti-virus software product must be installed on computer systems.

System Backups

1. All critical system software and data should be backed up onto removable media on a regular basis. The back-up media should then be stored off-site.
2. Incremental and full backups and protected backup storage will be maintained at the local level.
3. Sufficient server storage space or portable backup equipment will be provided to support end users.

Software Usage

The introduction of unauthorized or unlicensed software into FEMA's information processing environment is prohibited.

1. All FEMA employees must honor licenses, copyright laws and other measures designed to protect legitimate proprietary interests in computer software and data.
2. Users must not possess or use software or hardware tools that can be used to break security mechanisms. Examples of such tools are those that facilitate illegal copying of copy-protected software, that are used to discover secret passwords, or that are used for unauthorized decipherment of encrypted data.

Network Configuration Control

1. If a security breach occurs or a computer virus is discovered, the Network Administrator will identify and isolate the source of the problem and notify the ESM directly or through the ITSC.
2. The Network Administrator will maintain information detailing the current inventory, configuration, and connectivity of all equipment in their system(s). No network equipment will be added, removed or modified; and no computer connections to FEMA networks will be made without review and approval by the Network Administrator.

Remote Access (Dial-in and Dial-out)

1. Access to the FEMA enterprise network via the commercial dial phone system is a significant security risk. The connection of modems to the network without a security risk assessment and configuration control is prohibited.

2. No modem will be connected to any portion of the FEMA network without prior approval. Refer to Appendix 4-3.b, Remote Access using Hardware Tokens and TACACS, for detailed information.

3. All modems on the network will be under the configuration control of the National ITSC at Mt. Weather.

Left blank intentionally

4-4 Application Systems Life-Cycle Security Requirements

Overview

1. This chapter specifies safeguards for all major FEMA applications systems, that are by definition, large investments, mission critical, cross cutting, or high risk. Managers of major applications systems need to devote special attention to security due to the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of information in the system. These needs frequently extend beyond the scope of security procedures documented in this chapter. The procedures and controls discussed below present the minimum level of safeguards to be adopted.

2. All systems and applications require some level of security. The information systems safeguards presented in this chapter stress sound management controls. Technical and physical controls support sound management practices by extending the necessary security protection to systems and data. Security safeguards apply to both classified and unclassified information systems.

3. OMB Circular A-130, Appendix III, “Security of Federal Automated Information Systems,” requires Federal agencies to establish security controls in parallel with the application systems life-cycle process. The goal of these security controls is to ensure appropriate safeguards are incorporated into all new applications and into significant modifications to existing applications. The following safeguards include OMB Circular A-130 security control topics: assigning responsibility for security, security planning, review of security controls, and management authorization. The procedures also detail safeguards for ensuring security throughout the application systems life cycle. For more assistance or technical guidance, contact the FEMA Enterprise Security Manager.

Responsibility

1. The Chief Information Officer is responsible for:

   - Overseeing FEMA’s information systems security policy, procedures, and practices.

   - Identifying and affording security protections commensurate with the risk and magnitude of the harm that may result from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of the Agency.

   - Appointing FEMA’s Enterprise Security Manager.

   - Overseeing development and implementation of FEMA’s information security training program.

   - Approving recommendations for application systems security accreditation.

2. Executive Associate Director, Information Technology Services Directorate is responsible for:

   - Developing and implementing applicable information systems policy, procedures, standards, and guidelines on privacy, confidentiality, security, disclosure, and sharing of information collected, processed, transmitted, or maintained by or for the Agency.

   - Coordinating with the Executive Associate Director, Operations Support Directorate, on all security matters pertaining to classified and sensitive unclassified information systems.

3. Associate Directors, Administrators, Executive Associate Directors, Regional Directors, and Office Directors are responsible for:

   - Ensuring FEMA's information systems security policy, requirements, and guidelines are followed in developing system specifications and contracts for the acquisition or operation of information systems, associated resources, and facilities.

   - Issuing, for programs and functions under their purview, information systems safeguards beyond the Agency's minimum stated requirements, as required.

   - Assigning security personnel, Site Mangers/Administrators and/or Network Administrators, as required.

   - Conducting effective security certification and accreditation for major, mission critical, high risk, financial, or classified information systems.

   - Authorizing information systems and by implication accepting the risks extant in the systems.

   - Implementing controls consistent with the criticality, value, and sensitivity of the information being handled.

   - Ensuring that employees are made aware of all information security policies and procedures and that security training is available for users, custodians, and owners of sensitive FEMA information assets.

4. The Inspector General is responsible for:

   - Performing independent audits relating to information systems security, including assessing compliance with information systems security and privacy legislation, regulations, and requirements.

- Assisting the CIO and the Director, Security Division of the Operations Support Directorate, in information systems security investigations; or as appropriate, conducting criminal investigations and making referrals to the United States Department of Justice.

5. The FEMA Enterprise Security Manager is responsible for:

- Approving the acquisition, configuration and installation of routers, switches, firewalls and other network-related equipment.
- Assuring FEMA information assets are used only for FEMA purposes.
- Assuring compliance with all applicable State and Federal laws and administrative policies.
- Assuring compliance with security policies and procedures established by the owners of the information assets and by the FEMA CIO.
- Advising the owner of information and the CIO of any vulnerability presenting a threat to information assets, and for providing specific means of protecting that information.
- Notifying the owner of information and the CIO of any actual or attempted violations of security policies, practices or procedures.
- Approving the addition of Local Area Network (LAN) or Wide Area Network (WAN) devices that impact Internet or Intranet services.
- Establishing and approving the security configuration control of all network devices.
- Developing or assisting with the development of operational procedures.
- Assuring adherence to all FEMA WAN-naming conventions.
- Developing or assisting with the development of operational procedures.
- Assuring adherence to all FEMA WAN-naming conventions.
- Providing support for the issuance of hardware tokens and maintenance of authentication databases.
- Evaluating vendor security products and apprising the Agency of approved Information Technology (IT) security products and techniques.
- Developing security accreditation guidelines and procedures for new application development.

- Participating as technical security advisor on in-house system development projects and assisting with security control implementations.
- Performing independent audits relating to information systems security, including assessing compliance with information systems security and privacy legislation, regulations and requirements.
- Conducting pre-production security tests to ensure compliance with FEMA security practices for new applications and devices.
- Investigating reports of information systems security compromises, violations or breaches, and recommending or implementing security countermeasures or corrective actions, as appropriate.
- Performing other security duties as assigned.

6. The Site Manager/Administrator has overall responsibility for:

   - Managing the local networks at a location where there are multiple local area networks with different Network Administrators.
   - Ensuring security, integrity, availability, and confidentiality of local information systems and network services for the site.
   - Presenting security orientations to current employees and new hires.
   - Processing newly arriving and departing employees to ensure compliance with security procedures, as required in Chapter 4-4 under “Personnel Security and Control” and “Access Control” headings.

7. The Network Administrator is responsible for:

   - Establishing and maintaining configuration, operation and security of the local system.
   - Maintaining the configuration management of all hardware and software connected to the local network.
   - Ensuring that system/network users comply with IT security policies and procedures.
   - Reviewing and auditing the information system/network on a regular basis to determine that the network remains secure.
   - Reporting any suspected security incidents to FEMA’s Information Technology Service Center (ITSC) at Mt. Weather (540) 542-4000 or directly to the ESM.

- Ensuring the integrity of program data through regularly scheduled system backups and any required restorations.

8. The Information Technology Service Center (ITSC), which is located at Mt. Weather, is responsible for:

   - Providing 24-hour-a-day, 7-day-a-week help desk for users of FEMA's information systems during declared disasters. At other times, the ITSC operates 16 hours a day. The ITSC can be reached on (540) 542-4000.

   - Taking reports on and processing suspected or actual network security problems.

   - Notifying the ESM and appropriate system/network administrator immediately following the reported incident.

Procedures

<u>Personnel Security and Control</u>

1. <u>Separation of Duties</u>.

   Structure the application systems development or maintenance environment where possible, to implement the control principle of separating duties. This practice provides a system of checks and balances and minimizes opportunities for any one individual to circumvent established security controls and adversely affect an application system while it is under development or maintenance.

2. <u>Privileges</u>.

   - Include security-related responsibilities in job descriptions and performance plans for personnel involved in application systems development and maintenance.

   - Implement the principle of least privilege in the application systems development or maintenance environment (i.e., grant each individual only the minimum physical and system access privileges needed to perform assigned duties).

3. <u>Personnel Security</u>.

   - Ensure that adequate personnel security measures are implemented in the application systems development or maintenance environment by complying with applicable procedures of the Security Division of the Operations Support Directorate.

   - Depending on the sensitivity of the application system under development or maintenance, required security measures may include personnel security clearances, normal access authorizations, and access privileges and restrictions based on need to know or need to use.

4. Security Awareness Training.

   - Provide basic security awareness training to personnel involved in the development or maintenance of an application system. Relevant system and application security issues, threats, vulnerabilities, requirements, and responsibilities should be emphasized.
   - Develop application-specific security awareness training material as a security feature of the application system.
   - All personnel associated with the application system should be aware of the basics of information systems security and application-specific security issues, threats, vulnerabilities, countermeasures, and personal security responsibilities.
   - The Computer Security Act of 1987 requires all personnel involved with sensitive automated information systems, including managers, operators, and end-users, to receive basic awareness training in information systems security.
   - All FEMA end users and other personnel associated with FEMA systems are required to read and sign a security agreement. By signing the agreement, personnel acknowledge they have received, read, and understood FEMA information security policy, procedures, and practices.
   - Failure by personnel to comply with FEMA's security policies, procedures, and practices will be grounds for disciplinary action up to and including termination of employment or contracts.

Security Plan

1. Establish an application system security policy and plan for protecting each application system and its resources throughout the systems life cycle.
2. Define application system security and control objectives in the security policy and establish rules for accessing and using application system functions, data, and other resources based on the application's sensitivity, identified threats, vulnerabilities, and risks.
3. Establish a security plan for each sensitive application system. Follow OMB Bulletin No. 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information. Consult the FEMA Enterprise Security Manager to obtain additional guidance.
4. Document and maintain the application system security policy and plan as a permanent part of the application system documentation library.

Sensitivity Analysis

1. Perform application system sensitivity analysis early in the system development or maintenance process.

2. Analyze the nature and characteristics of application functions and data to determine the application's level of sensitivity in the areas of confidentiality, integrity, and availability.

3. Identify sensitive, critical, or powerful application system functions as the basis for defining functional access control and separation of duty requirements.

4. Review application data elements independently, in combination, and in the aggregate to determine the sensitivity or classification level of data processed by the application system as the basis for defining data access control requirements.

5. Consider the regulatory and policy framework surrounding the application to determine special requirements related to confidentiality, integrity, or availability.

6. Document the results of sensitivity analysis and maintain the documentation as a permanent part of the application system's documentation library.

Access Control

1. Define and document the access control security features of the application. Given identified subjects (users) or groups of subjects and given named objects (e.g., application functions, programs, transactions, accounts, data files, records, etc.), provide comprehensive predefined rules to determine which subjects or groups may be permitted access to a specific application object. Security clearance, formal access approval, and need to know or need to use must be considered in granting access to classified application systems and application objects. Need to know or need to use should be criteria in granting access to unclassified application systems and objects.

2. Incorporate an automated access control feature into the application's security design to assist in enforcing the access control policy. Physical and administrative control measures may be required to supplement automated controls.

3. Establish an access control level for the application commensurate with the sensitivity level of application functions and data. Some applications may require access control only at the program and data file level, while more sensitive applications may require intra-program functional access control or data access control at the record or field level.

4. Provide an access control mechanism that is capable of the following:

   - Denying access to all non-privileged users by default (i.e., denying access to all users initially and then permitting access to selected application users by authorized exception);

   - Supporting the principle of least privilege (i.e., supporting the capability of granting each user no more access to application functions and data than is absolutely necessary to perform assigned duties); and,

   - Supporting the principle of separating sensitive or critical application system duties, so no one individual user can have complete control over the application, adversely affect application resources, or use the application for personal gain. For instance, sensitive financial management system transactions should be independently originated, authorized, executed, and reconciled.

5. Integrate access control modes into the application security structure when necessary to provide a finer grain of control over application programs and data files.

6. Include documented, application-specific access control guidelines as a security feature of the application system to assist system managers, security administrators, and application managers in establishing an adequate access control structure for the application in an operational environment. Guidelines should identify sensitive or critical application functions, programs, and data objects requiring access restrictions on the basis of security clearance, formal access approval, need to know, or separation of duties. Additionally, guidelines should provide the detailed technical information that is necessary to configure the access control mechanism and enforce the application's access control policy.

7. Do not provide any application system feature or function that permits bypassing or requires disabling the access control mechanism.

8. Protect the access control mechanism and related data files from unauthorized access by non-privileged application users and other unauthorized personnel.

9. Access control for major mission-critical, cross cutting, or high-risk FEMA information systems should include the following procedures:

   - Develop a process whereby a user or a supervisor from a functional area such as a FEMA Directorate, Office, etc., enters and submits an automated system access request for approval by the appropriate supervisor.

   - Provide automated access for supervisors to approve or deny requests from users or supervisors under their purview.

- Provide for functional areas to designate authorizing officials with duties to review and approve or deny on behalf of the functional area requests for system access.
- The designated system administrator receives and reviews access requests, creates accounts, and notifies the functional areas, supervisors, and users.
- It is required that the functional area authorizing officials designate user accounts that are no longer required when their status changes and to certify at least quarterly to the system administrator that each user account is still needed.

The system administrator disables user accounts that are no longer required upon notification from functional area authorizing official's Risk Assessment.

1. Perform a basic risk assessment of each application system's processing and teleprocessing environment in light of the results of the application system sensitivity analysis. These results and the results of the risk assessment should provide the foundation for formulating application-specific security requirements (i.e., definitions of security features, both manual and automated, required to adequately protect application system resources).
2. Perform threat and vulnerability analysis as a means of assessing application system risks. Identify and assess the nature and extent of potential threat agents, threat effects on the application (e.g., unauthorized disclosure, modification, destruction of application software or data, hardware damage, delay or total denial of service, etc.), and vulnerabilities in the application's physical, system, and telecommunications environment.
3. Document the results of risk assessment and maintain the documentation as a permanent part of the application system's documentation library.

Security Requirements

1. Define application system security requirements during the requirements analysis and definition phase of the system's life-cycle process, or when major system change or enhancement requirements are formulated for an existing application system.
2. Consider the following when defining application system security requirements:

   - The nature and characteristics of application functions and data;
   - The results of application sensitivity analysis and risk assessment;
   - Federal laws, regulations, and standards, as well as FEMA policies and directives applicable to the application system's functionality, data, and level of sensitivity;
   - National security directives and FEMA information security policies and requirements when the application involves classified data processing, storage, or transmission; and

- Baseline application systems security feature requirements outlined in this document.

3. Document application system security requirements and maintain the documentation permanently in the application system's documentation library.

4. Submit security requirements to the application management for review and approval prior to beginning application system design.

Security Specifications

1. Define functional security specifications for the application system during the design phase of the system's life-cycle process. OMB Circular A-130 defines security specifications, as detailed descriptions of the safeguards required to protect an application.

2. Integrate security design specifications into the overall design of the application system.

3. Document security design specifications and maintain the documentation as a permanent part of the application system's documentation library. Security specification documentation should clearly relate design specifications to application security objectives and requirements to provide management assurance that specifications satisfy objectives and requirements.

4. Submit security design specifications to application management for review and approval prior to beginning formal development (programming) of the application system. OMB Circular A-130 requires security design reviews and management approval of application security design specifications.

System Protection

1. Base the extent of security control in the system development or maintenance environment on the sensitivity of the application system under development or maintenance. The more sensitive application functionality and/or data, the more essential it is to exercise continuous control over the system development or maintenance environment.

2. Ensure application system source code, object code, and authorized development or maintenance personnel can only access programming utilities resident on the system. Application code on the development or maintenance system should be protected against unauthorized disclosure, modification, and destruction through an access control mechanism that permits access only to identified, authenticated, and authorized personnel.

3. Conduct all system development or maintenance activities under closed shop or protective conditions. The development or maintenance system, system environment, and associated operations, as well as software and documentation products should be positively controlled with access granted only to authorized personnel. As noted above, the principle of least privilege should govern all access authorizations and activities.

4. Define and document system backup strategy and related procedures and assign backup responsibilities to protect software modules while under development or maintenance. Restrict backup and restore operations to a minimum number of authorized personnel and grant only authorized personnel physical access to areas used to store backup media.

Application System Design and Development

1. Use structured software engineering methodologies and techniques during system design, development, and maintenance to provide a controlled software-engineering environment resulting in reliable, maintainable, secure application system software. The use of structured techniques can produce modular software that supports security by isolating sensitive application system functions, which can be secured through an access control mechanism.

2. Do not design or program the application or any function in a way that permits system-level security controls to be circumvented or requires those controls to be disabled.

3. Do not design or program any mode of entry into the application system for maintenance, support, or operation that violates system or application-level security control features or permits bypassing those features (e.g., a trap door or back door designed to permit system development or maintenance personnel to bypass established access controls).

4. Do not design or program any mode of entry into the application system for maintenance, support, or operation unless it is an approved and documented feature of the application system.

5. Use structured walk-through (peer reviews) to identify and resolve potential security flaws in program design and code and to locate and remove trap doors or back doors and malicious code (computer viruses, time bombs, logic bombs, Trojan horses, etc.).

6. Do not hard code passwords or encryption keys in clear-text form in application system programs or data files.

7. Document and protect security-related code. This includes code that implements security features or mechanisms, code that performs highly sensitive or critical processing, and code that accesses highly sensitive or critical data during execution.

8. Review all changes to application system functional requirements, data requirements, and design specifications throughout the system's life-cycle process to determine whether corresponding changes are required in application system security requirements and specifications.

Audit and User Accountability

1. Incorporate an audit trail facility into the security design of the application to provide individual user auditability and accountability while on the system and operating within the application. The audit trail should be capable of associating and recording unique user IDs

with actions taken by individual application system users. For many applications, the audit trail facility provided by the operating system may be sufficient to provide application auditability and user accountability. Some applications, however, may require significantly enhanced audit capabilities (e.g., a financial management system). When additional audit capabilities are required, the application system itself or supporting software such as a database management system (DBMS) must address the requirement for an enhanced audit facility.

2. Provide an audit trail facility that is capable of the following:

   - Recording events and violations related to system log on, log off, and all changes to the security status of the system and application (i.e., all actions related to creating, modifying, or deleting data in system and application security files, including the audit trail file itself);

   - Selectively auditing and recording application events and violations related to application files opened for reading, opened for modification, renamed, or deleted, and application programs or procedures executed; and,

   - Recording the following information about events and violations: date, time, and user ID associated with events and violations recorded, type of event or violation (e.g., unauthorized attempt to open a file for modification), and descriptions of modifications made to security mechanisms and related data files.

3. Provide documented, application-specific guidelines for configuring and using the audit trail facility to monitor application system security and maintain individual user accountability.

4. Provide guidelines for reviewing and analyzing application audit trail data. Guidelines should include translations of programmer-defined application program and data file names into user-recognizable application functions and data names. This will assist in using the audit facility to detect unauthorized application access attempts, highly unusual patterns of authorized activity, or other anomalies that may indicate actual or potential security problems within the application.

5. Do <u>not</u> provide any application system feature or function that permits bypassing or requires disabling the audit trail mechanism.

6. Protect the audit trail facility and associated data files from access by non-privileged application users or other unauthorized personnel.

Input Controls

1. Design manual or automated input controls for the application system to ensure only authorized, valid, complete, and accurate source data is entered into the application system

database. Reliable input controls protect data integrity by ensuring authorized data is accurately converted into machine-readable form, not suppressed or lost, added to, duplicated, or otherwise improperly modified. Safeguards that reduce the potential for harmful effects from data entry errors or accidents (as opposed to deliberate acts) are a first step toward reducing opportunities for deliberate acts such as fraud or intentional misuse. An application that tolerates frequent errors is a fertile field for deliberate, malicious activities that can be masked as errors. Examples of input controls are:

- Source document preparation, review, and authorization procedures;
- Automated data validation techniques such as input screen validity checks, edit routines, or use of data dictionaries; and
- Manual or automated input reconciliation controls or procedures (e.g., comparing and reconciling system generated totals to manual control totals after data entry sessions).

2. Provide appropriate control procedures to protect sensitive application system source documents, if such documents are required by an application. For classified applications, protective measures for source documents must satisfy security requirements specified in FEMA Manual 1230.1.

Output Controls

1. Design security mechanisms and procedures to control output generated by the application system. Application output refers to printed reports and listings, the results of inquiries, displays on system terminals or workstations, and application data recorded on magnetic media or other types of storage media. Sensitive application system output should be appropriately controlled by manual or automated means to prevent unauthorized disclosure.
2. Provide application system security controls and procedures for producing, marking, handling, distributing and storing highly sensitive unclassified or classified application system output on electronic storage media, paper, or displayed on terminals or workstations.

Transmission Controls

1. Incorporate transmission security and control features into the application system's security design when the sensitivity of application data requires protection during transmission. Protection must be commensurate with the risk of disclosure, loss, misuse, alteration, destruction, or otherwise unavailable application system data.
2. Protect classified application data during transmission in accordance with communications security requirements specified in FEMA Manual 1200.5.
3. Employ encryption or other protection techniques, (message authentication, electronic certification or signature, etc.) approved by the National Institute of Standards and Technology, when unclassified data requires more than minimum protection to ensure data confidentiality or integrity during transmission.

Backup and Recovery

1. Provide a documented backup strategy and related procedures to protect against the loss or destruction of application software and data in the operational environment. Adequate application system backups of software and data are required to ensure the continuity of application system operations.

2. Design recovery features and provide associated procedures to permit recovery after system or application failure. If application system integrity and availability requirements dictate an increased level of protection in this area, incorporate automated recovery mechanisms such as those provided by DBMS technology (e.g., marking quiet points in the database, keeping a journal of before-and-after images, and using roll back and roll forward techniques to restore the integrity and availability of the application database).

3. Provide documented policies and procedures on archiving, retaining, and destroying application system data. In some application system areas, Federal or FEMA regulations may generate specific application systems requirements in these areas.

Contingency Planning

1. Develop, document, and maintain a contingency plan for the application system. A contingency plan consists of plans, procedures, arrangements, and required actions necessary to ensure the continuity of critical application system operations and the availability of application functions and data. OMB Circular A-130 requires a contingency plan as a security feature of each application system to ensure application users can continue to perform essential functions in the event that information technology support for the application is interrupted.

2. Address procedures and activities in the plan that ensure application system hardware, software, data, documentation, and other necessary application system items are readily available in backup form, should primary resources be damaged, lost, or destroyed.

3. Ensure the application system contingency plan is consistent with the disaster recovery or continuity of operations plan formulated for the facility or facilities where the application will be installed.

Security Tests

1. Test all security features incorporated into the application system. OMB Circular A-130 requires security testing prior to placing an application system into operation to ensure security controls function as designed and are operationally adequate.

2. Conduct security testing as part of the normal systems life-cycle testing process for new applications (i.e., during program or unit testing, system integration testing, and system acceptance testing).

3. Conduct security testing when an existing application is significantly modified or enhanced. Application system regression testing should include testing all existing security controls to ensure application changes and enhancements have not affected the functionality or reliability of these controls.

4. Conduct security testing in support of the OMB Circular A-130 requirement for application systems security certification. Security certification testing should be conducted as part of system testing or user acceptance testing for a new application or an existing application that has been significantly modified. Three types of testing are required in support of security certification:

   - Security feature functional testing to determine that specified security features exist, satisfy requirements and design specifications, and function properly;

   - Security feature performance testing to assess factors such as security feature reliability, availability, accuracy, response time, maintainability, ease of use, etc.; and,

   - Security feature penetration resistance testing to assess resistance against breaking or circumventing application system security controls.

5. Prepare security certification test documentation to include a security test plan, test scripts, and a test analysis report.

6. Maintain security certification test documentation as a permanent part of the application system documentation library.

<u>Security Certification and Accreditation</u>

1. Submit the application system to FEMA's Enterprise Security Manager for formal security certification and accreditation. Certification is the process of collecting, generating, and evaluating technical evidence as the basis for certifying that application system security features meet applicable Federal policies, regulations, and standards, and that test results demonstrate installed security safeguards are adequate for the application. Security certification is the technical basis for application system accreditation or formal management approval for operation in light of established security controls and residual risks.

2. Prepare a security certification report for the application system. Guidance on preparing the certification report is provided in FIPS PUB 102, Guideline for Computer Security Certification and Accreditation.

3. Maintain the security certification report as a permanent part of the application system documentation library.

4. Submit the security certification report and supporting application system security documentation to FEMA's Enterprise Security Manager for certification review prior to placing the application into operation. The Enterprise Security Manager shall evaluate application system security certification and conduct independent security reviews and assessments if additional certification evidence is required. If the application meets applicable Federal policies, regulations, and standards, and if security design reviews and test results demonstrate that security controls are adequate for the application; the Enterprise Security Manager shall recommend security accreditation to FEMA's Chief Information Officer.

Security Review and Recertification

1. Conduct security reviews or audits as the basis for recertification and reaccreditation of the application system. OMB Circular A-130 requires periodic review and recertification to evaluate the continued adequacy of implemented safeguards, to ensure all are still functioning properly, to identify new or modified threats and vulnerabilities, and to assist with the implementation of new security features where required.

2. Conduct security reviews or audits for recertification and reaccreditation:

   - At least every 3 years, or whenever an application system is significantly modified;

   - Whenever there are major changes in application system requirements, including changes in Federal or FEMA security policies or in user requirements related to security and control (as in the need to process data of a higher sensitivity or classification level); or

   - Whenever an application system security compromise, violation, audit, or risk assessment calls into question a prior security certification and accreditation.

3. Update the application system certification report and other security related documentation during the recertification process.

4. Maintain recertification documentation as a permanent part of the application system's documentation library.

5. Submit the recertification report and updated application security documentation package to the Enterprise Security Manager for recertification review and reaccreditation.

Configuration Management

1. Establish a configuration management system to authorize, control, and document changes to the application system hardware, software, and documentation baseline.

2. Maintain the configuration management system throughout the systems life-cycle process as prescribed in the FIRMPD, Chapter 2-4, Configuration Management.

3. Use the configuration management system to support security by ensuring application modifications and enhancements do not degrade the security posture of the application system.

Left blank intentionally